Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури.

І. Загальні положення

1. Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури, що здійснюють діяльність в Україні (далі – Методичні рекомендації), створено з метою оперативного виявлення кіберзагроз, кібератак, кіберінцидентів, визначення їх наслідків, мінімізації їх впливу та встановлення часу відновлення здійснення/надання критичних послуг/операцій, забезпечення планового рівня функціонування платіжної інфраструктури, підвищення надійності платіжних систем та захисту інтересів їх користувачів.

2. Методичні рекомендації розроблено відповідно до Законів України "Про Національний банк України", "Про платіжні системи та переказ коштів в Україні", Положення про нагляд (оверсайт) платіжних систем та систем розрахунків в Україні, затвердженого постановою Правління Національного банку України від 28 листопада 2014 року № 755 (зі змінами), з урахуванням кращої міжнародної практики, принципів та провідних міжнародних документів щодо забезпечення кіберстійкості інфраструктури фінансового ринку.

3. Національний банк рекомендує об'єктам платіжної інфраструктури дотримуватися цих Методичних рекомендацій, а Центральному депозитарію цінних паперів, системам розрахунків у цінних паперах, центральним контрагентам та торговим репозиторіям брати їх до уваги під час своєї діяльності з метою забезпечення кіберстійкості.

4. Методичні рекомендації передбачають такі ключові принципи діяльності платіжної інфраструктури:

1) чіткі та прозорі механізми управління;

2) надійна структура управління ризиками;

3) остаточність розрахунків;

4) регламентованість процедур, спрямованих на виявлення загроз, зменшення їх впливу та оперативне відновлення діяльності;

5) виявлення, моніторинг та управління ризиками в екосистемі платіжної інфраструктури.

5. Значення термінів, які вживаються в цих Методичних рекомендаціях:

1) екосистема платіжної інфраструктури – сукупність усіх елементів об'єктів платіжної інфраструктури та взаємозв'язків і залежностей, що виникають між ними. До екосистеми платіжної інфраструктури можуть належати банки, платіжні організації платіжних систем, учасники платіжної

системи, оператори послуг платіжної системи, розрахунковий(і) банк(и), інші об’єкти інфраструктури фінансового ринку, з якими встановлено зв’язки;

2) інформаційні системи платіжної інфраструктури – сукупність інформаційно-комунікаційних технологій, програмних, апаратно-технічних та технологічних засобів і обладнання та/або інших засобів, призначених для обробки інформації в платіжній інфраструктурі;

3) керівники (керівництво) об’єктів платіжної інфраструктури – голова, його заступники та члени ради; голова, його заступники та члени правління; головний бухгалтер та його заступники;

4) кіберінцидент об’єкта платіжної інфраструктури (далі – кіберінцидент) – подія або ряд несприятливих подій, що ставлять під загрозу конфіденційність, цілісність, доступність інформації в платіжній інфраструктурі та/або захищеність її інформаційних систем у кіберпросторі та/або порушують передбачену політику та процедури, спрямовані на забезпечення кібербезпеки в платіжній інфраструктурі внаслідок навмисних злочинних або ненавмисних дій;

5) ландшафт кіберзагроз – сукупність існуючих та потенційних кіберзагроз для діяльності платіжної інфраструктури;

6) мережа об’єкта платіжної інфраструктури – комплекс технічних засобів телекомунікацій, призначених для обробки, зберігання, передавання та/або приймання даних між кінцевим обладнанням у платіжній інфраструктурі;

7) об’єкти платіжної інфраструктури – банки, платіжні організації платіжних систем, учасники/члени платіжних систем (далі – учасники платіжних систем), клірингові та процесингові установи, оператори послуг платіжної інфраструктури, міжнародні платіжні системи, платіжними організаціями яких є нерезиденти, у частині їх діяльності на території України;

8) оперативна інформація про кіберзагрози – зібрана, оброблена, інтерпретована, доповнена та готова до використання з метою прийняття управлінських рішень інформація про потенційні кіберзагрози;

9) оцінка вразливостей кіберстійкості платіжної інфраструктури (далі – оцінка вразливостей) – метод оцінки кіберстійкості платіжної інфраструктури, що полягає у систематичній експертизі інформаційної системи та засобів її контролю і процесів з метою визначення адекватності заходів безпеки, виявлення недоліків, надання даних для прогнозування ефективності запропонованих заходів безпеки та підтвердження їх адекватності після реалізації;

10) привілейований користувач – користувач, який має більше прав порівняно з іншими користувачами інформаційних систем платіжної інфраструктури;

11) толерантність до кіберризику – встановлені межі допустимого рівня кіберризику в платіжній системі;

12) фішинг – метод соціальної інженерії, що передбачає розсилання електронною поштою листів та/або створення вебсайтів, що вводять у оману користувачів інформаційних систем, та має на меті розголошення персональних даних, кодів/паролів та/або інших конфіденційних даних;

Інші терміни, які вживаються в цих Методичних рекомендаціях, використовуються в значеннях, визначених законами України та нормативно-правовими актами Національного банку України (далі – Національний банк).

ІІ. Безперервність діяльності платіжної інфраструктури

6. Метою управління безперервністю діяльності платіжної інфраструктури є забезпечення відповідного рівня обслуговування навіть у випадку, якщо відбувся інцидент в системі під час виконання стандартного розрахункового процесу.

7. Об’єкт платіжної інфраструктури має забезпечити спроможність своєчасно та ефективно виконувати/надавати критичні операції/послуги в штатному режимі діяльності платіжної інфраструктури та в надзвичайних ситуаціях.

8. Об’єкту платіжної інфраструктури рекомендується забезпечити ключові елементи управління безперервністю діяльності платіжної інфраструктури, якими є:

1) розроблення та затвердження стратегії безперервності діяльності;

2) визначення кіберінцидентів (природні катастрофи, припинення подання електроенергії, терористичні акти тощо), настання яких впливає на безперервність діяльності платіжної інфраструктури;

3) створення робочих груп з управління процесами у разі настання кіберзагроз, кіберінцидентів та кібератак, що можуть мати вплив на безперервність діяльності платіжної інфраструктури;

4) можливість швидко забезпечити відновлення діяльності на базі обладнання, розміщеного в іншому місці.

9. Об’єкту платіжної інфраструктури рекомендується забезпечити дотримання вимог Національного банку щодо організаційних та технічних заходів для забезпечення безперервності діяльності платіжної інфраструктури, а саме:

1) створення детальної схеми комплексу програмно-апаратних засобів із описом функціонального призначення та взаємозв’язку його компонентів;

2) визначення переліку критично важливих компонентів комплексу програмно-апаратних засобів та особливо важливих даних, необхідних для надання послуг, та запровадження політики їх резервування й відновлення;

3) забезпечення роботи критично важливих компонентів комплексу програмно-апаратних засобів джерелами безперебійного електроживлення;

4) здійснення резервного копіювання баз даних та інших особливо важливих даних;

5) забезпечення моніторингу всіх компонентів комплексу програмно-апаратних засобів, реєстрації та аналізу інцидентів, пов’язаних із порушенням безперервності діяльності;

6) забезпечення дотримання вимог законодавства України у сфері інтелектуальної власності під час використання програмного забезпечення на всіх компонентах комплексу програмно-апаратних засобів;

7) зберігання електронних архівів, архівів особливо важливих даних, а також програмних засобів, необхідних для відновлення змісту баз даних, на зовнішніх носіях щонайменше в одному примірнику в приміщенні за основним місцезнаходженням та додаткового примірника в приміщенні (кімнаті), територіально віддаленому(ній) від основного;

8) здійснення аналізу можливих загроз безперервному функціонуванню комплексу програмно-апаратних засобів, забезпечення мінімізації їх можливого впливу та планування дій для випадків їх можливої реалізації;

9) розроблення інструкцій дій обслуговуючого персоналу щодо попередження порушень у разі настання надзвичайної ситуації та відновлення функціонування комплексу програмно-апаратних засобів, їх аналіз та перегляд не рідше одного разу на рік;

10) забезпечення наявності інструкцій із супроводження та експлуатації комплексу програмно-апаратних засобів;

11) навчання обслуговуючого персоналу стосовно питань супроводження та експлуатації комплексу програмно-апаратних засобів і дій для відновлення його функціонування;

12) визначення порядку внесення змін до програмного забезпечення та конфігурації всіх компонентів комплексу програмно-апаратних засобів;

13) забезпечення обслуговування та технічної підтримки [надання консультацій користувачам (уключаючи проблеми, що виникли під час експлуатації), ремонт та заміна непрацюючого обладнання, установлення оновлень/нових версій та виправлення помилок програмного забезпечення] усіх компонентів комплексу програмно-апаратних засобів;

14) забезпечення взаємодії та комунікацій із користувачами та зацікавленими особами у разі виникнення надзвичайної ситуації.

ІІІ. Збереження даних у платіжній інфраструктурі

10. Структура та зміст даних, що створюються під час діяльності об’єктів платіжної інфраструктури, визначаються технологією роботи їх інформаційних систем та внутрішніми документами об’єкта платіжної інфраструктури.

11. Приміщення для зберігання даних рекомендується обладнати згідно з вимогами Національного банку до серверних приміщень і приміщень електронних архівів банків.

12. Об’єкту платіжної інфраструктури рекомендується забезпечити зберігання кількох копій даних, що створюються в платіжній інфраструктурі.

13. Вибір електронних носіїв для зберігання даних рекомендується здійснювати з урахуванням:

1) терміну зберігання даних;

2) надійного строку зберігання даних на електронному носії;

3) можливості переміщення носіїв до спеціально обладнаних місць зберігання.

14. Обладнання та програмне забезпечення, які використовуються платіжною інфраструктурою, мають забезпечувати роботу з усіма електронними носіями та форматами запису, що використовуються/використовувалися під час запису даних.

15. Об’єкту платіжної інфраструктури рекомендується проводити перевірки цілісності носіїв із даними, створеними в процесі діяльності платіжної інфраструктури, не рідше одного разу на рік.

16. Електронні носії з даними, створеними в процесі діяльності платіжної інфраструктури, рекомендується промаркувати для ідентифікації змісту та строків їх експлуатації та не менше як за три місяці до закінчення строку експлуатації здійснити перезапис цих даних на інший носій. Під час копіювання електронного документа з електронного носія обов’язково має бути виконана перевірка цілісності, достовірності та авторства даних на цьому носії.

17. Надання працівникам об’єкта платіжної інфраструктури доступу до таких даних рекомендується здійснювати на підставі їх документально оформлених запитів згідно з погодженням керівника підрозділу інформаційних технологій.

IV. Аналіз специфіки діяльності платіжної інфраструктури

18. Ефективність заходів, що вживаються об’єктом платіжної інфраструктури з метою забезпечення кіберстійкості платіжної інфраструктури, залежить від урахування специфіки її діяльності.

19. Об’єкту платіжної інфраструктури (в особі відповідального за управління кіберризиком) рекомендується здійснювати аналіз специфіки діяльності платіжної інфраструктури з метою виявлення найуразливіших до впливу кіберзагроз, кіберінцидентів та/або кібератак елементів і тих, які є критично важливими та насамперед потребують захисту.

20. Об’єкту платіжної інфраструктури для надання послуг рекомендується постійно здійснювати аналіз, актуалізацію та класифікацію платіжної інфраструктури за ступенем критичності та зазначати про це в своїх внутрішніх

документах із зазначенням ступеня критичності кожного з таких складових елементів платіжної інфраструктури:

1) операції/послуги;

2) процеси;

3) інформаційні ресурси (на основі схеми комплексу програмно-апаратних засобів, що створюється об'єктом платіжної інфраструктури відповідно до вимог, установлених нормативно-правовими актами Національного банку з питань оверсайта);

4) робота працівників, виконання обов'язків яких впливає на здійснення/надання послуг платіжної інфраструктури;

5) зовнішні взаємозв'язки та взаємозалежність об'єктів платіжної інфраструктури тощо (далі – елементи платіжної інфраструктури).

Виконання дій, передбачених у цьому пункті, рекомендується забезпечувати за допомогою автоматизованих систем/інструментів.

21. Об'єкту платіжної інфраструктури рекомендується аналізувати зовнішні взаємозв'язки та залежність із (від):

1) елементами (ів) екосистеми платіжної інфраструктури;

2) постачальниками (ів) послуг (електроживлення, телекомунікацій) та продуктів (програмного забезпечення, інформаційних технологій тощо);

3) кредиторами (ів) (за наявності) тощо.

22. Об'єкту платіжної інфраструктури під час створення схеми комплексу програмно-апаратних засобів відповідно до вимог, установлених нормативно-правовими актами Національного банку з питань оверсайта, рекомендується зазначати IP-адреси, призначені для адміністрування та супроводження інформаційних систем, мережевого обладнання, серверів, що використовуються для виконання/надання критичних операцій/послуг.

23. Об'єкту платіжної інфраструктури рекомендується здійснювати оцінку потенційних кіберризиків перед упровадженням нових послуг/операцій, технологій, взаємозв'язків у діяльності платіжної інфраструктури та враховувати результати здійсненої оцінки під час перегляду Положення про кіберстійкість.

V. Забезпечення кіберстійкості платіжної інфраструктури

24. Під забезпеченням кіберстійкості платіжної інфраструктури слід розуміти розроблені та впроваджені об'єктом платіжної інфраструктури підходи до управління кіберризиками.

25. Об'єкту платіжної інфраструктури рекомендується визначити особу, відповідальну за управління кіберризиком, включити її до складу виконавчого органу управління та забезпечити їй доступ до інформації та ресурсів (у тому

числі трудових) у обсязі, необхідному для виконання покладених на неї обов'язків.

26. Особа, відповідальна за управління кіберризиком, повинна мати знання, навички, професійний досвід у обсязі, необхідному (достатньому) для розуміння всіх аспектів діяльності платіжної інфраструктури, адекватної оцінки кіберризиків, прийняття виважених рішень, а також забезпечення ефективного управління та контролю з урахуванням покладених на неї обов'язків.

До таких обов'язків належать:

1) супроводження та надання консультації щодо розроблення внутрішніх документів, спрямованих на досягнення кіберстійкості платіжної інфраструктури, контроль та відповідальність за їх реалізацію і дотримання їх вимог;

2) консультування членів керівництва об'єкта платіжної інфраструктури в разі виникнення питань, пов'язаних із управлінням операційними ризиками в платіжній інфраструктурі та досягненням кіберстійкості платіжної інфраструктури; моніторинг та участь у заходах, що можуть мати вплив на досягнення кіберстійкості платіжної інфраструктури;

3) участь у розробленні плану дій у випадку надзвичайних ситуацій у частині питань, пов'язаних із забезпеченням кіберстійкості;

4) ініціювання та здійснення моніторингу впровадження заходів щодо забезпечення кіберстійкості;

5) розслідування кіберінцидентів (у межах компетенції) та звітування про них керівництву об'єкта платіжної інфраструктури;

6) здійснення на постійній основі аналізу кіберзагроз у діяльності об'єктів платіжної інфраструктури;

7) ініціювання та координація заходів щодо підвищення обізнаності та навчання персоналу об'єкта платіжної інфраструктури стосовно досягнення кіберстійкості платіжної системи;

8) участь у визначенні керівництвом об'єкта платіжної інфраструктури достатності трудових, технічних, матеріальних та інших ресурсів для досягнення кіберстійкості та своєчасне інформування керівництва об'єкта платіжної інфраструктури про виявлену недостатність таких ресурсів;

9) звітування (не рідше одного разу на три місяці) керівництву об'єкта платіжної інфраструктури про стан справ щодо досягнення кіберстійкості платіжної інфраструктури, у тому числі надання оцінки ситуації щодо кіберстійкості платіжної інфраструктури порівняно з попереднім звітним періодом, інформації про заходи, пов'язані з досягненням кіберстійкості платіжної інфраструктури, кіберінциденти та результати тестів на проникнення, тестів із залученням "червоних" команд.

27. Об'єкту платіжної інфраструктури необхідно забезпечити особу, відповідальну за управління кіберризиком, інформацією в обсязі, необхідному для виконання покладених на неї обов'язків, та необхідними ресурсами (у тому числі трудовими).

28. Об’єкту платіжної інфраструктури додатково рекомендується залучати зовнішні незалежні професійні організації або експертів із кіберризиків для вирішення окремих питань щодо кіберстійкості платіжної інфраструктури.

29. Об’єкту платіжної інфраструктури рекомендується розробити/доопрацювати з урахуванням цих Рекомендацій стратегію та політику щодо забезпечення кіберстійкості платіжної інфраструктури (далі – Положення про кіберстійкість).

30. Положення про кіберстійкість має бути погоджене особою, відповідальною за управління кіберризиком, та затверджене керівником, його заступником або виконавчим органом управління об’єкта платіжної інфраструктури.

31. Об’єкт платіжної інфраструктури під час розроблення та перегляду Положення про кіберстійкість має враховувати:

специфіку управління персоналом на об’єкті платіжної інфраструктури, а також процесів і технологій, що застосовуються в платіжній інфраструктурі;

результати аналізу операцій/послуг об’єктів платіжної інфраструктури тощо за ступенем їх критичності для платіжної інфраструктури;

кіберінциденти, що вже виникали під час діяльності платіжної інфраструктури;

висновки, отримані за результатами перевірок, аудиту, оцінювання платіжної інфраструктури;

інформацію про наявні та потенційні кіберзагрози, у тому числі ті, про які об’єкту платіжної інфраструктури стало відомо від зацікавлених осіб та з відкритих джерел;

стратегічні цілі діяльності та розвитку платіжної інфраструктури.

32. Об’єкту платіжної інфраструктури рекомендується, зокрема, визначати в Положенні про кіберстійкість платіжної інфраструктури:

1) важливість забезпечення кіберстійкості для платіжної інфраструктури та зацікавлених осіб;

2) цілі щодо забезпечення кіберстійкості платіжної інфраструктури та рівень толерантності до кіберризику;

3) пріоритетність застосування сучасних технологій для досягнення кіберстійкості платіжної інфраструктури;

4) порядок взаємодії об’єкта платіжної інфраструктури із зацікавленими особами, іншими суб’єктами інфраструктури фінансового ринку тощо з питань обміну інформацією;

5) порядок ідентифікації, механізми контролю, заходи щодо управління, мінімізації кіберризику та відновлення після кібератак;

6) особливості інтеграції питань кіберстійкості платіжної інфраструктури з ключовими процесами діяльності об’єкта платіжної інфраструктури, такими як:

забезпечення операційної діяльності;

управління персоналом;

експлуатація обладнання й інформаційних систем тощо;

7) використання в своїй діяльності міжнародних стандартів та рекомендацій, кращих практик у сфері забезпечення кіберстійкості;

8) розподіл функцій, обов'язків та повноважень між посадовими особами та органами управління щодо забезпечення кіберстійкості в платіжній інфраструктурі;

9) розподіл обов'язків, відповідальності та порядок звітування, у тому числі за прийняття рішень щодо ідентифікації, мінімізації, контролю та управління кіберризиком.

33. Об'єкту платіжної інфраструктури рекомендується забезпечувати перегляд, актуалізацію та оцінку ефективності реалізації Положення про кіберстійкість не рідше одного разу на рік, а також після виникнення кібератак на платіжну інфраструктуру та/або виявлення нових критичних залежностей.

34. Об'єкт платіжної інфраструктури самостійно визначає цілі щодо забезпечення кіберстійкості платіжної інфраструктури, які мають узгоджуватися з загальною політикою об'єкта платіжної інфраструктури щодо управління операційним ризиком у платіжній інфраструктурі, якими можуть бути, зокрема:

мінімізація впливу кіберзагроз, кіберінцидентів та кібератак на кіберстійкість платіжної інфраструктури та безперервність її діяльності;

забезпечення протидії та попередження кіберзагрозам, кіберінцидентам та кібератакам на платіжну інфраструктуру;

відновлення виконання/надання критичних операцій/послуг не пізніше ніж через дві години після виникнення кіберінциденту або кібератаки (або в інший визначений термін);

забезпечення злагоджених, заздалегідь визначених дій персоналу платіжної інфраструктури та суб'єктів її екосистеми в разі виникнення кіберінциденту та/або кібератаки;

35. Толерантність до кіберризику полягає у визначенні такого рівня кіберризику, на який платіжна інфраструктура погоджується.

Толерантність до ризику може мати:

1) високий рівень, який характеризується запровадженням та реалізацією мінімальних заходів з управління кіберризиком або їх відсутністю;

2) помірний рівень, який характеризується комплексним підходом до запровадження та реалізації платіжною інфраструктурою заходів, спрямованих на управління кіберризиком, та збалансованим інвестуванням у кіберстійкість платіжної інфраструктури;

3) нульовий рівень, що характеризується відносно високим рівнем застосування проактивних та превентивних дій для забезпечення кіберстійкості платіжної інфраструктури та інвестування в кіберстійкість з метою мінімізації кіберризиків.

36. Аналіз толерантності до кіберризику передбачає якісну та/або кількісну оцінку.

Кількісними параметрами толерантності до кіберризику можуть бути:

1) розмір збитків, які платіжна інфраструктура готова понести внаслідок кіберінциденту та/або кібератаки, що дозволить їй відновити та продовжувати виконання/надання критичних операцій/послуг у встановлені нею терміни. Зазначений показник ураховує власні кошти платіжної інфраструктури (резервний фонд), відшкодування, передбачене страхуванням тощо;

2) кількість допустимих кіберінцидентів та/або кібератак на платіжну інфраструктуру в установлений період;

3) тривалість припинення виконання/надання критичних операцій/послуг у зв'язку з кіберінцидентом та/або кібератакою (упродовж окремого кіберінциденту та/або кібератаки або у визначений період (наприклад, упродовж місяця, року) тощо.

Якісними параметрами толерантності до кіберризику можуть бути процеси, технології, персонал, вплив кіберінцидентів та/або кібератак, які не дозволять продовжувати виконання/надання критичних операцій/послуг.

37. Керівництво об'єкта платіжної інфраструктури може використовувати параметри толерантності до кіберризику в якості індикаторів, що вказують на адекватність реалізації заходів, спрямованих на забезпечення кіберстійкості платіжної інфраструктури.

38. Об'єкту платіжної інфраструктури рекомендується визначити в статутних та/або інших внутрішніх документах такі обов'язки її органів управління:

1) призначення особи, відповідальної за управління кіберризиком;

2) контроль за реалізацією Положення про кіберстійкість;

3) визначення достатності трудових, технічних, матеріальних та інших ресурсів для досягнення кіберстійкості платіжної інфраструктури та вжиття необхідних заходів у разі виявлення недостатності ресурсів для забезпечення належного рівня кіберстійкості платіжної інфраструктури;

4) пряму взаємодію особи, відповідальної за управління кіберризиком, із керівними органами платіжної інфраструктури та її(їх) незалежність, у тому числі від структурних підрозділів(осіб), відповідальних за розроблення, упровадження, супроводження (адміністрування) та експлуатацію інформаційних систем платіжної інфраструктури, забезпечення операційної діяльності платіжної інфраструктури та незалучення її до діяльності, пов'язаної з внутрішнім аудитом об'єкта платіжної інфраструктури;

5) надання особі, відповідальній за управління кіберризиком, повноважень щодо участі у формуванні бюджету, необхідного для проведення навчання в сфері кіберстійкості;

6) установлення вимоги до всіх співробітників об'єкта платіжної інфраструктури, що забезпечують діяльність платіжної інфраструктури,

звітувати уповноваженій особі про будь-які інциденти, що можуть мати вплив на кіберстійкість платіжної інфраструктури;

7) обізнаність персоналу платіжної інфраструктури щодо потенційних кіберзагроз, їх можливого впливу на платіжну інфраструктуру, заходів безпеки (наприклад, засобами електронної пошти або шляхом розміщення відповідної інформації на внутрішньому вебсайті об'єкта платіжної інфраструктури);

8) навчання персоналу платіжної інфраструктури (у тому числі керівників) щодо реагування на кіберзагрози, ландшафту кіберзагроз, нових тактик та методів кіберзагроз тощо та здійснення контролю за їх ефективністю (не рідше одного разу на рік);

9) додаткове навчання в сфері кіберстійкості платіжної інфраструктури посадових осіб об'єкта платіжної інфраструктури та інших осіб, що мають доступ до інформації з обмеженим доступом щодо діяльності платіжної інфраструктури.

VI. Захист платіжної інфраструктури від кіберзагроз, кіберінцидентів та кібератак

39. Досягнення кіберстійкості платіжної інфраструктури, серед іншого, залежить від ефективності заходів, спрямованих на запобігання, обмеження впливу та наслідків кіберзагроз, кіберінцидентів та кібератак на платіжну інфраструктуру.

40. Заходи, передбачені об'єктом платіжної інфраструктури для захисту платіжної інфраструктури від кіберзагроз, кіберінцидентів та кібератак на неї (далі – заходи захисту платіжної інфраструктури), мають базуватися на аналізі специфіки діяльності платіжної інфраструктури, проведеному відповідно до рекомендацій, наданих у розділі IV цих Методичних рекомендацій, та бути пропорційними визначеним ступеням критичності для надання послуг у платіжній інфраструктурі.

41. Заходи захисту платіжної інфраструктури мають передбачати, зокрема:

1) захист інформаційних ресурсів платіжної інфраструктури;

2) захист від ризиків, що виникають унаслідок установлених взаємозв'язків;

3) захист критично важливих елементів платіжної інфраструктури до, під час та після впровадження змін у діяльності платіжної інфраструктури;

4) захист від внутрішніх загроз, джерелом яких є персонал платіжної інфраструктури;

5) навчання персоналу з питань кіберстійкості;

6) фізичну безпеку об'єкта платіжної інфраструктури та її персоналу, необхідну для забезпечення кіберстійкості платіжної інфраструктури.

42. Заходи захисту платіжної інфраструктури мають забезпечувати, зокрема:

1) безперервне, надійне функціонування та доступність інформаційних систем платіжної інфраструктури;

2) цілісність інформації, що зберігається та/або передається через інформаційні системи платіжної інфраструктури;

3) захищеність, конфіденційність, цілісність та доступність даних, що зберігаються та/або передаються в платіжній інфраструктурі;

4) відповідність діяльності вимогам законодавства та міжнародним стандартам.

43. Об'єкту платіжної інфраструктури під час упровадження заходів захисту платіжної інфраструктури рекомендується застосовувати багаторівневий підхід до забезпечення кіберстійкості платіжної інфраструктури (Defence-in-Depth). Багаторівневість полягає в упровадженні багаточисельних та диференційованих рівнів фізичного, технічного, логічного захисту платіжної інфраструктури, захисту від внутрішнього шахрайства з боку персоналу платіжної інфраструктури та інших видів захисту платіжної інфраструктури, які перешкоджають подальшому проникненню загроз у разі вразливості заходів захисту нижчих рівнів.

44. Об'єкту платіжної інфраструктури рекомендується забезпечити реалізацію заходів захисту платіжної інфраструктури, зазначених у пунктах 45 – 49 цих Рекомендацій.

45.Заходи, пов'язані з управлінням мережею та інфраструктурою платіжної інфраструктури:

1) розроблення та впровадження системи захисту інформації, що має базуватися на комплексі загальноприйнятих міжнародних стандартів (ISO 27001, ISO 20000-1, ISO 27103 тощо);

2) розподіл мережі платіжної інфраструктури (сегментація мережі, поділ мережі на менші мережі) відповідно до ризиковості окремих сегментів та політики безпеки, що застосовується до них;

3) розподіл інформаційного середовища платіжної інфраструктури (баз даних, серверів тощо) та операцій/послуг платіжної інфраструктури із забезпеченням відповідного рівня їх безпеки та заходів контролю;

4) забезпечення технічних заходів для запобігання доступу за неавторизованим кодом до пристроїв, що належать об'єкту платіжної інфраструктури або управляються ним, мережевої інфраструктури та компонентів системи;

5) упровадження технічних заходів та засобів для запобігання підключенню неавторизованих пристроїв до мережі платіжної інфраструктури;

6) застосування автоматизованих механізмів для підтримання повноти забезпечення актуальності налаштувань та конфігурацій безпеки інформаційних систем та їх компонентів;

7) використання для управління загрозами таких інструментів як міжмережевий екран (firewall), система запобігання несанкціонованому доступу

до мережі (Intrusion Prevention System, IPS), система виявлення несанкціонованого доступу до мережі (Intrusion Detection System, IDS), віртуальна приватна мережа (Virtual Private Network, VPN, закритий для сторонніх за допомогою шифрування канал обміну інформацією), демілітаризована зона (DMZ, особливий сегмент мережі, в якому обмежено доступ до серверів із публічної мережі) тощо;

8) відмова від адміністрування засобів захисту мережі та інших складових інформаційних систем безпосередньо з мереж загального користування та, за можливості, заборона прямого доступу з пристроїв або серверів, що використовуються для адміністрування інформаційних систем, до мережі Інтернет;

9) установлення у внутрішніх документах об'єкта платіжної інфраструктури вимог щодо налаштувань та конфігурацій безпеки інформаційних систем, у тому числі щодо пристроїв, які використовуються для віддаленого доступу до мережі платіжної інфраструктури, та дотримання їх в актуальному стані;

10) відслідковування та контроль на постійній основі нетипової активності користувачів, а також змін у налаштуваннях та/або конфігураціях системи захисту інформації та програм, що можуть уносити такі зміни (у тому числі щодо пристроїв, які використовуються для віддаленого доступу до мережі платіжної інфраструктури);

11) використання захищених мережевих криптографічних протоколів [наприклад, Secure Shell та протоколи, налаштовані на захист транспортного рівня (Transport Layer Security, TLS) або їх еквіваленти] для забезпечення конфіденційності та цілісності інформації, обмін якою здійснюється;

12) установлення граничного терміну бездіяльності (неактивності) користувачів та інших умов (за необхідності), після настання/виконання яких обмежуються, блокуються та припиняються віддалені сеанси роботи та впровадження процедур для реалізації зазначених заходів;

13) застосування спеціальних засобів для попередження, виявлення та блокування кіберзагроз та/або кібератак на пристроях, що використовуються об'єктом платіжної інфраструктури, зокрема тих, що використовуються віддалено (антивіруси, мережеві екрани, системи виявлення та/або запобігання вторгненням до мережі платіжної інфраструктури тощо);

14) моніторинг застарілих інформаційних систем платіжної інфраструктури, оцінка їх уразливості, та (за необхідності) запровадження додаткових рівнів заходів захисту та/або встановлення оновлень, що усувають виявлені вразливості;

15) розроблення та застосування політики та засобів контролю, які запобігають установленню працівниками неавторизованих програм та додатків;

46.Фізичні та логічні заходи захисту платіжної інфраструктури:

1) упровадження автоматичної системи контролю та сповіщення особи, відповідальної за управління кіберризиком, про дії користувачів інформаційних ресурсів, що виходять за межі наданих їм прав доступу;

2) упровадження автоматичної системи відключення та/або видалення неактивних, тимчасово створених облікових записів, що не використовуються.

3) забезпечення обмеження фізичного та логічного доступу працівників до інформаційних систем платіжної інфраструктури на рівні, необхідному для якісного виконання ними своїх службових обов'язків;

4) установлення обмежень щодо прав фізичного, логічного та/або віддаленого доступу до критично важливих інформаційних систем та блокування несанкціонованого доступу, а також регулярний перегляд таких прав;

5) упровадження рольової системи контролю доступу [Role-based Access Control (RBAC)], а саме:

забезпечення групування користувачів інформаційних ресурсів відповідно до ролей (функцій), які вони виконують у платіжній інфраструктурі, (наприклад, керівні органи, персонал, відповідальний за управління ризиками, адміністратори операційних систем, учасники платіжної системи тощо), та встановлення стандартних прав, повноважень, привілеїв щодо доступу в інформаційних системах для користувачів інформаційних ресурсів, що належать до визначених груп;

створення, адміністрування облікових записів користувачів інформаційних ресурсів, а також надання прав, повноважень та привілеїв відповідно до приналежності користувача інформаційних ресурсів за його функціональними обов'язками до встановленої групи;

призначення співробітників, відповідальних за перегляд актуальності визначених ролей та їх групування;

забезпечення перегляду відповідальним(и) співробітником(ами) актуальності визначених ролей та їх групування, у тому числі щодо привілейованих користувачів інформаційних ресурсів (груп користувачів), не рідше одного разу на рік;

здійснення контролю за відповідністю наданих користувачам інформаційних ресурсів, у тому числі привілейованим (групам користувачів), повноважень та прав доступу на мінімально необхідному рівні для якісного виконання ними своїх службових обов'язків, не рідше одного разу на рік,

своєчасне виявлення та обмеження (скасування) повноважень та прав доступу до інформаційних систем для користувачів інформаційних ресурсів, у тому числі привілейованих, що перевищують мінімально необхідний рівень для якісного виконання персоналом своїх службових обов'язків;

6) забезпечення наявності окремих облікових записів адміністраторів операційних систем для вирішення адміністративних завдань щодо інформаційних систем платіжної інфраструктури та виконання інших функцій (за потреби), забезпечення їх ідентифікації;

7) установлення вимог щодо автентифікації користувачів інформаційних ресурсів (наприклад, паролі, смарт-карти, біометричні дані тощо), що відповідають стандартам (наприклад, NIST-800-63);

8) розроблення засобів контролю доступу до даних, що зберігаються та передаються в платіжній інфраструктурі (наприклад, шифрування, автентифікація, контроль доступу);

9) розроблення заходів для запобігання несанкціонованому доступу та політики доступу до криптографічних ключів та інших засобів криптографічного захисту інформації;

47. Заходи захисту платіжної інфраструктури, пов'язані з унесенням змін до програмного забезпечення платіжної інфраструктури та їх оновленням (далі у цьому підпункті – зміни):

1) автоматизація процесу управління змінами;

2) створення та застосування спеціального середовища, що відповідає операційному середовищу об'єкта платіжної інфраструктури, для попереднього оперативного тестування змін та, за необхідності, забезпечення відмови від упровадження окремих змін;

забезпечення наявності політики, процедур, засобів контролю та управління змінами, які встановлюють критерії пріоритетності та класифікація таких змін;

3) до унесення змін рекомендується здійснити аналіз відповідності змін потребам діяльності платіжної інфраструктури; виявлення та аналіз ризиків, що виникають унаслідок змін та їх негативний вплив на забезпечення конфіденційності, цілісності, доступності інформації в платіжній інфраструктурі; обов'язкове схвалення запланованих змін виконавчим органом об'єкта платіжної інфраструктури;

4) залучення особи, відповідальної за управління кіберризиком та/або інших працівників, залучених до забезпечення кіберстійкості платіжної інфраструктури, на всіх етапах упровадження змін у діяльності платіжної інфраструктури;

5) упровадження процедур, які підтверджують відсутність помилок та ефективність упровадження змін [наприклад, аналіз програмного коду (Code Review) та модульне тестування (unit testing, перевірка коректності роботи окремих модулів програмного коду)];

6) тестування, документування та схвалення змін у інформаційних системах платіжної інфраструктури, зокрема модифікація апаратного, програмного забезпечення або компонентів програмного забезпечення та налаштування системи та системи безпеки до моменту їх упровадження;

7) наявність затверджених процесів ідентифікації, оцінки та схвалення термінових (екстрених) позапланових змін;

8) проведення аналізу після впровадження термінових (екстрених) позапланових змін на предмет коректності їх упровадження та оцінки наслідків;

9) застосування, за можливості, стандартних налаштувань інформаційних систем/технологій, що застосовуються в платіжній інфраструктурі, у процесі унесення змін;

10) передбачення процедури оперативного відновлення у разі, якщо впроваджені зміни мали негативні наслідки;

11) запровадження політики та процедури, що не дозволяють уносити зміни, що не були схвалені в установленому порядку.

48. Заходи захисту платіжної інфраструктури, пов’язані з управлінням персоналом:

1) упровадження автоматичної системи контролю та сповіщення відповідального(их) за надання прав доступу в інформаційних системах платіжної інфраструктури працівника про кадрові рішення, які потребують зміни/відміни таких прав (звільнення, переведення тощо);

2) упровадження заходів захисту платіжної інфраструктури до кожного з етапів управління персоналом, зокрема:

здійснення необхідних перевірок службою безпеки кандидата на посаду до прийняття на роботу;

забезпечення дотримання працівниками та залученими для надання окремих послуг особами встановленої політики, процедур та засобів контролю щодо кіберстійкості;

установлення вимоги щодо повернення пристроїв, що надають доступ до інформаційних систем, особами, яких звільнено або відсторонено від виконання обов’язків;

3) установлення політики, процедур та заходів контролю за наданням, зміною та скасуванням прав фізичного та логічного доступу працівників до інформаційних систем платіжної інфраструктури, необхідних для якісного виконання персоналом службових обов’язків;

4) регулярний перегляд прав фізичного та логічного доступу працівників до інформаційних систем платіжної інфраструктури;

5) моніторинг та контроль активності привілейованих користувачів та користувачів, що мають доступ до критично важливих інформаційних ресурсів платіжної інфраструктури, з метою виявлення нетипової активності та протиправних дій з їх боку;

49. Заходи захисту платіжної інфраструктури, пов’язані із захистом від ризиків, що виникають унаслідок установлених взаємозв’язків:

1) розроблення та упровадження заходів захисту для виявлення та запобігання несанкціонованим вторгненням до мережі платіжної системи внаслідок встановлених взаємозв’язків;

2) наявність процедур, що дозволяють ізолювати або блокувати (тимчасово) встановлені взаємозв’язки у разі кібератаки та/або кіберінциденту;

3) незалежний аудит процесів, пов’язаних із наданням послуг або виконанням функцій у платіжній інфраструткурі операторами послуг платіжної інфраструктури;

4) перевірка кіберстійкості операторів послуг платіжної інфраструктури, наприклад, шляхом зовнішнього аудиту *(за міжнародним стандартом ISAE 3402)*, укладення угод про рівень обслуговування (Service Level Agreements, SLAs) тощо;

5)співпраця з операторами послуг платіжної інфраструктури з метою удосконалення забезпечення кіберстійкості платіжної інфраструткури;

6) регулярний перегляд списку учасників платіжної системи, операторів послуг платіжної інфраструктури та постачальників послуг та врахування їх під час розроблення заходів захисту від кіберризиків, що виникають унаслідок установлених взаємозв'язків;

7) постійна оцінка ризиків, що виникають унаслідок установлених взаємозв'язків, та встановлення відповідності реалізації переданих функцій рекомендаціям щодо забезпечення кіберстійкості платіжної інфраструктури, встановленим цими Методичними рекомендаціями;

8) установлення вимоги до операторів послуг платіжної інфраструктури, що обслуговують платіжну інфраструктуру, щодо необхідності здійснення самооцінювання відповідно до вимог, установлених у Додатку F міжнародних стандартів "Принципи для інфраструктур фінансового ринку", з використанням відповідної методики[1].

50. Об'єктам платіжної інфраструктури рекомендується не рідше одного разу на рік здійснювати контроль ефективності заходів захисту та переглядати їх з метою адаптації вимог щодо налаштувань та конфігурацій безпеки інформаційних систем до ландшафту кіберзагроз.

VII. Управління кіберризиком

51. У цьому розділі надаються рекомендації об'єктам платіжної інфраструктури з управління кіберризиком стосовно складової операційного ризику, що призводить до порушень в управлінні кіберризиком унаслідок зовнішніх подій.

52. Питання управління кіберризиком об'єкта платіжної інфраструктури мають бути віднесені до компетенції органу, в складі якого мають бути представники керівництва та/або керівник об'єкта платіжної інфраструктури, а також необхідний персонал для розроблення та впровадження стратегії управління кіберризиком і основ забезпечення кібербезпеки.

53. Стратегія управління кіберризиком має враховувати такі положення:

1) важливість кібербезпеки для об'єкта платіжної інфраструктури та ключових зацікавлених сторін;

2) вимоги внутрішніх і зовнішніх зацікавлених сторін для визначення цілей та заходів з управління кіберризиком;

3) візію та місію об'єкта платіжної інфраструктури щодо кібербезпеки;

4) цілі кібербезпеки для об'єкта платіжної інфраструктури, які мають містити постійне забезпечення ефективності, результативності та економічної життєздатності послуг для клієнтів об'єкта платіжної інфраструктури, а також підтримку і підвищення здатності передбачати, протистояти, стримувати кіберінциденти та кібератаки та відновлюватися після їх настання;

[1] Assessment methodology for the oversight expectations applicable to critical service providers, CPSS-IOSCO, 2014

5) межі впливу на об’єкт платіжної інфраструктури можливих кіберризиків для гарантування їх сумісності з цілями стратегії управління кіберризиком, а також із загальними бізнес-цілями і корпоративною стратегією об’єкта платіжної інфраструктури;

6) дорожню карту або план реалізації з плануванням можливостей, пов’язаних із людьми, процесами й технологіями, відповідно до кіберризиків. Стратегія має чітко визначати, як буде здійснюватися ця дорожня карта або план реалізації, і як керівництво об’єкта платіжної інфраструктури має відстежувати й контролювати його виконання;

7) перелік технологій і активів та їх необхідний рівень для забезпечення управління кіберризиками;

8) порядок взаємодії між об’єктами платіжної інфраструктури та третіми сторонами в таких сферах як обмін інформацією;

9) порядок управління, необхідний для розроблення, експлуатації та підвищення ефективності кібербезпеки;

10) порядок реалізації та фінансування ініціатив із забезпечення кібербезпеки, включаючи, за можливості, процес формування бюджету об’єкта платіжної інфраструктури з питань управління кіберризиком;

11) порядок інтегрування управління кіберризиком в усі аспекти діяльності об’єкта платіжної інфраструктури, включаючи персонал, процеси, технології та нові бізнес-ініціативи.

54. Об’єкт платіжної інфраструктури має забезпечити відповідність стратегії управління кіберризиком своїй корпоративній стратегії та іншим стратегіям (наприклад, стратегії управління ризиками установи, управління операційним ризиком та ІТ-ризиком).

55. Керівництво об’єкта платіжної інфраструктури має забезпечити регулярний перегляд стратегії, аналіз та оновлення відповідно до ландшафту кіберризиків.

56. Керівництво об’єкта платіжної інфраструктури має регулярно отримувати інформацію про кіберризики для досягнення загальних бізнес-цілей і цілей корпоративної стратегії.

VIII. Виявлення кіберзагроз, кіберінцидентів та кібератак на платіжну інфраструктуру

57. Спроможність об’єкта платіжної інфраструктури виявляти кіберзагрози, кіберінциденти та кібератаки на ранній стадії дозволяє своєчасно вжити необхідних заходів реагування та знизити їх негативний вплив на діяльність платіжної інфраструктури.

58. З метою своєчасного виявлення кіберзагроз, кіберінцидентів та кібератак на платіжну інфраструктуру об’єкта платіжної інфраструктури рекомендується:

1) визначити та встановити у внутрішніх документах типовий профіль активності користувачів із метою виявлення нетипової активності, яка не

відповідає встановленій політиці безпеки платіжної інфраструктури, та подій кібербезпеки;

2) забезпечити необхідні кадрові, технічні та інші ресурси для здійснення моніторингу активності користувачів та надавачів послуг і виявлення нетипової активності та подій кібербезпеки, розробити та запровадити автоматизацію такого моніторингу;

3) установити відповідні умови, критерії, параметри тощо, за умови виникнення яких відбувається сповіщення про виявлення нетипової активності та подій кібербезпеки;

4) використовувати інформацію, зібрану під час моніторингу активності користувачів та надавачів послуг, для подальшого удосконалення процесу моніторингу їх активності та процедури реагування на кіберінциденти та кібератаки;

5) запровадити використання спеціального програмного забезпечення для фіксації та аналізу інформації, отриманої в результаті сповіщення про події кібербезпеки, з метою постійного моніторингу інформаційного середовища платіжної інфраструктури (наприклад, баз даних, серверів та точок, в яких платіжна інфраструктура може наражатися на ризики в сфері кібербезпеки тощо) та виявлення нетипової активності користувачів та кіберінцидентів і кібератак;

6) переглядати не рідше одного разу на рік та, за необхідності, оновлювати типовий профіль активності користувачів і надавачів послуг, а також критерії, параметри тощо, за умови виникнення яких відбувається сповіщення про події кібербезпеки;

7) проводити необхідні тренування для забезпечення спроможності персоналу об’єкта платіжної інфраструктури ідентифікувати та повідомляти про нетипову активність і події кібербезпеки;

8) упровадити багаторівневі заходи виявлення кібератак та ізоляції вражених ділянок, що мають охоплювати персонал, процеси та технології;

9) використовувати інформацію щодо кіберзагроз, отриману з будь-яких джерел, відповідно до рекомендацій, наданих у розділі VI цих Методичних рекомендацій, під час упровадження заходів, передбачених для виявлення кіберзагроз, кіберінцидентів та кібератак на платіжну інфраструктуру;

10) збирати та зберігати інформацію, отриману під час моніторингу активності користувачів та надавачів послуг, із забезпеченням резервного копіювання даних та зберігання їх у захищеному місці із забезпеченням неможливості унесення змін до них;

11) здійснювати постійний моніторинг рівня кіберризиків на всіх стадіях життєвого циклу інформаційних ресурсів платіжної інфраструктури, зберігати та аналізувати отриману інформацію, а також використовувати її для своєчасного реагування на кіберзагрози та дослідження нетипової активності користувачів;

12) здійснювати моніторинг та перевірку Інтернет-трафіка, у тому числі в разі віддаленого доступу, налаштувань і активності в потенційних точках нараження платіжної інфраструктури на кіберризики з метою вчасного виявлення потенційних уразливостей та нетипових подій;

13) забезпечувати порівняння фактичного Інтернет-трафіка та налаштувань у потенційних точках нараження платіжної інфраструктури на кіберризики з очікуваним Інтернет-трафіком та стандартними налаштуваннями.

IX. Реагування на кіберінциденти та кібератаки на платіжну інфраструктуру та відновлення її діяльності

59. Об'єкту платіжної інфраструктури рекомендується передбачити план дій на випадок кіберінцидентів та кібератак на платіжну систему та порядок відновлення діяльності, які повинні базуватися на аналізі специфіки діяльності платіжної інфраструктури, проведеному відповідно до рекомендацій, зазначених у розділі IV цих Рекомендацій.

60. Об'єкту платіжної інфраструктури рекомендується забезпечити реалізацію заходів захисту платіжної інфраструктури, зазначених у пунктах 61 – 65 цих Рекомендацій.

61. Заходи захисту платіжної інфраструктри, пов'язані з управлінням кіберінцидентами:

1) з урахуванням ступенів критичності операцій/послуг, процесів, інформаційних ресурсів та зовнішніх взаємозвязків і залежностей платіжної інфраструктури:

визначити цільові точки відновлення, які вимірюються в одиницях часу (секунди, хвилини, години). Цільова точка відновлення визначає періодичність створення в платіжній інфраструктурі резервних копій даних та момент, з якого повинна бути відновлена інформація в платіжній інфраструктурі після порушення безперервності діяльності платіжної інфраструктури/виникнення кіберінциденту для відновлення її діяльності;

установити час відновлення діяльності платіжної інфраструктури, який вимірюється в одиницях часу. Цільовий час відновлення діяльності платіжної системи визначає плановий період часу після порушення безперервності діяльності платіжної інфраструктури/виникнення кіберінциденту, впродовж якого надання послуг платіжною інфраструктурою має бути відновлене;

2) регулярно розглядати різні сценарії кіберінцидентів та кібератак на платіжну інфраструктуру, що включають екстремальні, але ймовірні події, та аналізувати їх можливий вплив на діяльність платіжної інфраструктури;

3) розробити план(и) реагування на кіберінциденти, спрямований(і) на досягнення цільової точки відновлення та час відновлення діяльності платіжної інфраструктури, в якому(их) необхідно:

визначити ролі та відповідальність за відновлення діяльності платіжної інфраструктури, а також у разі загострення ситуації;

мінімізувати негативні наслідки кіберінцидентів та/або кібератак;

визначити пріоритетність дій щодо поновлення та відновлення діяльності платіжної інфраструктури;

мати на меті спрощення оброблення критичних операцій/послуг, підвищення довіри зацікавлених осіб та скорочення витрат на відновлення діяльності платіжної інфраструктури;

передбачити альтернативні варіанти для зміни (переорієнтування) критично важливих елементів платіжної інфраструктури, що відповідно до передбачених сценаріїв потенційно можуть бути уражені на тривалий період часу.

4) сформувати команди реагування на кіберінциденти/кібератаки, члени яких повинні мати необхідні знання та навички для вирішення кіберінцидентів;

5) установити спеціальні параметри для виявлення кіберінцидентів, за якими відбуватиметься передавання інформації відповідальним особам та реалізація заходів реагування;

6) забезпечити регулярне тестування плану(ів) реагування, поновлення та відновлення діяльності платіжної інфраструктури щодо передбачених сценаріїв кіберінцидентів та кібератак на платіжну інфраструктуру;

7) установити процеси і процедури:

зіставлення та перегляду інформації, передбаченої планом(ами) реагування, поновлення й відновлення діяльності платіжної інфраструктури з фактичними наслідками кіберінцидентів, а також результатами тестування, та застосування їх для удосконалення відповідного(их) плану(ів);

аналізу причин, що призвели до кіберінцидентів/кібератак, та використання результатів аналізу для розроблення та удосконалення плану(ів) реагування, поновлення та відновлення діяльності платіжної інфраструктури;

8) здійснити детальний аналіз прийняття рішень щодо поновлення здійснення операцій/надання послуг, ураховуючи, що критично важливим є забезпечення завершення розрахунків упродовж операційного дня;

9) розробити сценарії на випадок неможливості відновлення діяльності платіжної інфраструктури протягом двох годин після виникнення кіберінциденту;

10) упровадити заходи, спрямовані на виявлення, аналіз, стримування та відновлення платіжної інфраструктури після кіберінцидентів на ранньому етапі (до виникнення суттєвих порушень у діяльності платіжної інфраструктури). Такі заходи можуть, у тому числі, передбачати наявність прямих договірних відносин із установами, що надають відповідні послуги;

11) визначити та розробити функціональні схеми, а також схеми залежностей критичних функцій від інформаційних ресурсів платіжної інфраструктури та пріоритети їх відновлення;

12) ураховувати досвід, отриманий унаслідок кіберінцидентів інших суб'єктів управління кіберризиком у платіжній інфраструктурі, для удосконалення планів реагування, відновлення, передбачених об'єктом платіжної інфраструктури;

13) проводити консультації із зацікавленими особами (у тому числі з учасниками платіжної системи, операторами послуг платіжної інфраструктури) у межах екосистеми платіжної інфраструктури з метою розвитку та

удосконалення плану(ів) реагування та відновлення, передбаченому (их) об’єктом платіжної інфраструктури;

14) забезпечувати постійний моніторинг, оцінку та врахування нових технологічних розроблень та технологічних рішень, які можуть удосконалити можливості щодо реагування на кіберінциденти та відновлення діяльності платіжної інфраструктури;

62. Заходи захисту платіжної інфраструктури, пов’язані із забезпеченням цілісності даних:

1) розроблення та встановлення у внутрішніх документах об’єкта платіжної інфраструктури політики та процедури резервного копіювання даних, що включає періодичність та обсяг резервного копіювання;

2) упровадження методів та стратегії резервного копіювання, що дозволять обмежити порушення та відновити системні операції з мінімальними затримками;

3) забезпечення регулярного збереження (резервування) даних у захищеній резервній робочій зоні, що має інший, ніж основна робоча зона, профіль ризику даних, необхідних для поновлення трансакцій учасників;

4) захист резервних копій під час зберігання та передавання для забезпечення їх конфіденційності, цілісності та доступності даних, а також систематична перевірка доступності та цілісності резервних копій;

5) забезпечення реалізації інформаційними системами об’єкта платіжної інфраструктури механізмів відновлення трансакцій.

63. Заходи захисту платіжної інфраструктури, пов’язані із забезпеченням комунікації та співробітництва:

1) установлення, визначення та регулярний перегляд систем та процесів підтримки критичних функцій та / або операцій, які залежать від зовнішніх взаємозв’язків, у внутрішніх документах об’єкта платіжної інфраструктури;

2) розроблення політики та процедур, що визначають порядок співпраці з відповідними пов’язаними особами для забезпечення відновлення послуг/операцій (пріоритетними є критичні функції та послуги/операції) у безпечний і зручний час.

3) тісна співпраця з іншими суб’єктами управління кіберризиком у платіжній інфраструктурі та встановлення процесу скасування змін, унесених під час транзакції (до початку транзакції або точки збереження), та регулярна перевірка ефективності таких процедур;

4) розроблення інфраструктури мережевого підключення таким чином, щоб під час виникнення кібератаки з’єднання миттєво розривалося (здійснювалося сегментування мережі), із забезпеченням безперервності надання послуг під час розриву одиничних з’єднань.

64. Заходи захисту платіжної інфраструктури, пов’язані з комунікаціями під час надзвичайної ситуації та несанкціонованим розкриттям інформації:

1) визначення відповідальних осіб, які мають критичне значення для зниження ризику виникнення кіберінцидентів, та доведення до їх відома інформації щодо їх ролі та відповідальності залежно від рівня загострення ситуації;

2) визначення переліку зацікавлених осіб, яких необхідно повідомити в разі виникнення інциденту, а також обсягу інформації, що надається у повідомленні, та строків її надання;

3) розроблення та впровадження механізму негайного повідомлення вищого керівництва об'єкта платіжної інфраструктури, відповідного персоналу та заінтересованих осіб (уключаючи Національний банк та інші уповноважені органи) про кіберінциденти через належні канали комунікації з відстеженням руху повідомлення та підтвердженням інформації щодо отримання такого повідомлення. Механізм негайного повідомлення має здійснюватися відповідно до заздалегідь установлених критеріїв сповіщення з урахуванням досвіду;

4) установлення критеріїв та процедур, відповідно до яких питання щодо вирішення кіберінцидентів та усунення вразливостей діяльності платіжної інфраструктури уноситимуться на розгляд керівних органів/керівника платіжної інфраструктури, з урахуванням потенційних наслідків та їх критичності для діяльності платіжної інфраструктури;

5) розроблення плану комунікацій та процедур для своєчасного повідомлення внутрішніх та зовнішніх зацікавлених осіб, у тому числі Національного банку, засобів масової інформації та користувачів послуг платіжної інфраструктури, про виникнення кіберінциденту;

6) установлення політики та процедур щодо розкриття інформації про потенційну вразливість платіжної інфраструктури з метою сприяння оперативному реагуванню заінтересованими особами на кіберризики та зниження можливості його поширення на екосистему платіжної інфраструктури;

7) установлення та регулярний перегляд правил, угод та засобів контролю за публікацією та розповсюдженням інформації щодо кіберінцидентів;

8) вжиття заходів для запобігання розкриттю та розповсюдженню інформації, поширення якої може мати негативні наслідки для діяльності платіжної інфраструктури.

65. Заходи захисту платіжної інфраструктури, пов'язані із забезпеченням готовності до судових експертиз:

1) визначення даних, що можуть слугувати доказами під час судових експертиз;

2) виявлення та документування даних у інформаційних системах, що можуть слугувати доказами під час судових експертиз, а також їх розміщення та забезпечення належного їх оброблення впродовж всього життєвого циклу;

3) розроблення та впровадження політики/засобів щодо підготовки до судових процесів, у тому числі ведення системних журналів (із уточненням їх типів, періодів зберігання). Об'єкт платіжної інфраструктури може залучати для проведення такої підготовки спеціалістів на умовах аутсорсингу;

4) установлення політики безпечного зберігання доказів, що дозволить забезпечити їх достовірність та цілісність;

5) установлення процедур для можливості (за потреби) демонстрації цілісності збереження доказів та відстеження послідовності дій із ними в будь-який момент виникнення необхідності доступу до них, під час їх використання або переміщення;

6) проведення навчання працівників правилам поводження з доказами з метою уникнення інцидентів, пов'язаних із неможливістю їх використання у якості доказу;

7) залучення до проведення розслідувань працівників, що мають необхідні знання та навички для роботи з доказами та можуть забезпечити їх автентичність і цілісність, із урахуванням вимог до доказів, встановлених законодавством України.

8) забезпечення інтеграції політики/засобів щодо підготовки до судових процесів із планами з управління інцидентами та іншими планами;

9) установлення процедур удосконалення політики/засобів щодо підготовки до судових процесів

X. Тестування ефективності заходів, спрямованих на забезпечення кіберстійкості платіжної інфраструктури

66. Тестування є невід'ємним елементом будь-яких процесів, спрямованих на забезпечення кіберстійкості платіжної інфраструктури, що дозволяє виявити її недоліки та встановити напрями вдосконалення.

67. Об'єкту платіжної інфраструктури для забезпечення належного тестування ефективності заходів, спрямованих на забезпечення кіберстійкості платіжної інфраструктури, рекомендується:

1) запровадити з урахуванням ризик-орієнтованого підходу комплексну програму тестування (за необхідності, переглядати/оновлювати її), яка має складатися з методології, практики та інструментів для моніторингу, оцінювання та встановлення ефективності ключових компонентів механізму/системи забезпечення кіберстійкості платіжної інфраструктури;

2) залучити під час розроблення та впровадження програми тестування представників усіх зацікавлених підрозділів (уключаючи підрозділи, що забезпечують операційну діяльність);

3) забезпечити незалежність осіб, що проводять тестування (як внутрішніх, так і зовнішніх);

4) запровадити політику та процедури для визначення пріоритетності проблем/недоліків, виявлених за результатами проведення тестів, та шляхів їх вирішення/усунення з подальшим контролем якості відповідних дій;

5) періодично перевіряти доступність і читабельність резервних копій, що створюються в платіжній інфраструктурі;

6) проводити не рідше одного разу на рік тестування:

критичних систем, програм та планів відновлення даних;

планів реагування та відновлення, передбачених об’єктом платіжної інфраструктури, включаючи управління, координацію та комунікації під час їх реалізації;

7) забезпечити цілісність програми тестування та інших процесів управління ризиками, передбачених у платіжній інфраструктурі, та виявлення, аналіз і фіксація вразливості в кібербезпеці, що виникають унаслідок упровадження нових послуг або встановлення нових взаємозв’язків;

8) забезпечити можливості для пошуку, аналізу та використання оперативної інформації про кіберзагрози для оновлення своєї програми тестування та забезпечення її відповідності сучасному ландшафту кіберзагроз та методам дій зловмисників;

9) застосовувати кращі практики та автоматизовані інструменти для підтримки процесів та процедур, установлення технічних та організаційних вразливостей, виявлених під час тестування та перевірки на відповідність затвердженим політикам і конфігураціям;

10) здійснювати тестування та оцінки безпеки на всіх стадіях життєвого циклу інформаційних ресурсів платіжної інфраструктури та на будь-якому рівні для всього портфеля програм, включаючи мобільні додатки;

68. Об’єкту платіжної інфраструктури рекомендується забезпечити реалізацію таких заходів, пов’язаних з оцінкою вразливостей кіберстійкості платіжної інфраструктури:

1) розроблення, документальне затвердження та систематичне оновлення процесів управління вразливостями, що передбачає їх класифікацію, визначення пріоритетності та шляхів усунення, а також подальший контроль за якістю усунення виявлених вразливостей;

2) виявлення під час управління вразливостями будь-яких експлуатаційних недоліків (технічних, технологічних, організаційних або таких, що виникають несподівано) у критичних функціях, процесах, що їх підтримують, а також задіяних інформаційних ресурсах;

3) проведення регулярного сканування вразливостей внутрішніх систем, мереж та сторонніх сервісів, що використовуються в платіжній інфраструктурі;

4) проведення оцінки вразливостей, ураховуючи діючі процеси управління змінами, перед упровадженням нових/зміною існуючих служб/сервісів, які забезпечують підтримку критичних функцій, програм та компонентів інфраструктури;

5) періодична оцінка вразливостей послуг, програм та компонентів інфраструктури, оцінка їх відповідності політиці та правилам, установленим у платіжній інфраструктурі, та оцінка ефективності заходів, передбачених для усунення виявлених вразливостей;

6) проведення постійного сканування вразливостей спеціальними апаратними або програмними засобами за змінних умов з метою забезпечення комплексного сканування впродовж року;

69. Об’єкту платіжної інфраструктури рекомендується забезпечити реалізацію таких заходів, пов’язаних зі стрес-тестуванням кіберстійкості платіжної інфраструктури:

1) залучення під час тестування керівних органів та керівників вищої ланки (за необхідності);

2) обов’язкове застосування сценаріїв стрес-тестування, що передбачають соціальну інженерію та фішингові симуляції (з метою поліпшення обізнаності персоналу та підвищення культури управління ризиками в межах платіжної інфраструктури) ;

3) перевірка адекватності процесів, процедур та реагування персоналу на екстремальні, але ймовірні події;

4) тестування плану (ів) реагування, поновлення та відновлення, передбаченого(их) об’єктом платіжної інфраструктури, на базі сценарію, що передбачає:

знищення, втрату, пошкодження цілісності даних;

недоступність систем та даних;

значні фінансові втрати;

одночасний негативний вплив на декілька елементів екосистеми платіжної інфраструктури;

5) співпраця в межах екосистеми платіжної системи під час розроблення сценаріїв кіберінцидентів для проведення стрес-тестування з метою кращого розуміння поширення та передавання ризиків у платіжній інфраструктурі.

70. Об’єкту платіжної інфраструктури рекомендується не рідше одного разу на рік забезпечити реалізацію проведення з урахуванням ризик-орієнтованого підходу тестів на проникнення внутрішніх систем та мереж, та сторонніх сервісів, що використовуються у платіжній інфраструктурі.

71. Під час проведення тестів на проникнення всіх критично важливих внутрішніх та зовнішніх зацікавлених осіб рекомендується включати в тестування учасників/акціонерів об’єкта платіжної інфраструктури та осіб, відповідальних за забезпечення безперервності діяльності платіжної інфраструктури та реагування на інциденти.

XI. Ситуаційна обізнаність та обмін інформацією про кіберінциденти

72. Платіжна інфраструктура може суттєво підвищити кіберстійкість завдяки забезпеченню високого рівня своєї ситуаційної обізнаності та екосистеми платіжної інфраструктури в цілому. Ключовим засобом забезпечення ситуаційної обізнаності є активне налагодження домовленостей щодо обміну інформацією в сфері кіберризиків та співпраця у цій сфері.

73. Об’єкту платіжної інфраструктури рекомендується визначити кіберзагрози, які потенційно можуть мати негативний вплив на:

1) спроможність платіжної інфраструктури своєчасно та ефективно виконувати/надавати критичні операції/послуги;

2) спроможність об'єкта платіжної інфраструктури виконувати свої зобов'язання;

3) екосистему платіжної інфраструктури в цілому.

74. Об'єкту платіжної інфраструктури рекомендується забезпечувати аналіз інформації про кіберзагрози, отриманої з різних джерел, із урахуванням специфіки діяльності платіжної системи та з метою:

оцінки вірогідності цілеспрямованої атаки на платіжну інфраструктуру;

оцінки вразливості операційних систем, програмного забезпечення тощо і можливість їх використання для здійснення кібератак на платіжну інфраструктуру;

аналізу наявної інформації про кіберінциденти в інших платіжних інфраструктурах, їх учасниках, а також інших установах (типи кібератак, їх мета, джерела, періодичність, потенційний ризик для платіжної інфраструктури тощо).

75. Об'єкту платіжної інфраструктури для забезпечення високого рівня ситуаційної обізнаності рекомендується:

1) забезпечити можливості для збору інформації про кіберзагрози з внутрішніх та зовнішніх джерел [наприклад, використовуючи журнали програм, систем та мереж, міжмережеві екрани (firewall), системи виявлення вторгнень (IDSs), доступну інформацію];

2) вжити заходів для отримання доступу до наявних ресурсів обміну інформацією про кіберзагрози та вразливості (така інформація має містити аналіз тактик та процедур, що використовують зловмисники, їх методів дій, інформацію про геополітичні події, які можуть зумовити кібератаки на будь-який елемент екосистеми платіжної інфраструктури);

3) постійно використовувати отриману інформацію про кіберзагрози для посилення кіберстійкості платіжної інфраструктури;

4) забезпечувати наявність актуальної інформації про кіберзагрози, необхідної для прийняття рішень;

5) на постійній основі використовувати інформацію про кіберзагрози для передбачення можливих намірів та дій зловмисників та кібератак;

6) розробити, постійно оновлювати та уносити на розгляд керівних органів інформаційну панель (у формі графіків, таблиць тощо) щодо кіберзагроз (Cyber Threat Risk Dashboard), що містить:

перелік суб'єктів, що потенційно становлять загрозу для кіберстійкості платіжної інфраструктури;

узагальнений та деталізований опис поведінки (тактик, технік та процедур) зловмисників;

ймовірність кібератаки з боку визначених суб'єктів та можливий вплив на конфіденційність, цілісність та доступність даних у платіжній інфраструктурі та її репутацію в цілому внаслідок таких атак;

наслідки та вплив кібератак, що вже відбулися, на екосистему платіжної інфраструктури;

заходи, спрямовані на зниження вірогідності та управління потенційною кібератакою;

7) включити до переліку кіберзагроз загрози, що можуть зумовити екстремальні, але ймовірні події, навіть, якщо вони є малоймовірними та ніколи не виникали в минулому.

76. Об'єкту платіжної інфраструктури для належного обміну інформацією про кіберзагрози рекомендується:

1) визначити цілі та завдання щодо обміну інформацією, а саме своєчасний збір та обмін нею з метою своєчасного виявлення кібератак на платіжну інфраструктуру, а також забезпечення належного реагування, поновлення та відновлення від них;

2) визначати об'єм та вид інформації, що підлягає обміну, умови, за яких відбувається обмін інформацією, та її подальше використання, а також коло осіб, з якими можливий обмін інформацією (наприклад, учасники платіжної системи, оператори послуг платіжної інфраструктури та інші зацікавлені особи);

3) установити та регулярно оновлювати правила обміну та домовленості щодо обміну інформацією, враховуючи необхідність захисту потенційно чутливих даних, розкриття яких може призвести до порушення кіберстійкості платіжної інфраструктури та/або інших негативних наслідків;

4) визначити та встановити надійні та безпечні канали для обміну інформацією;

5) забезпечити можливості для своєчасного обміну інформацією із зацікавленими особами як у межах екосистеми платіжної інфраструктури, так і поза нею (наприклад, наглядові та правоохоронні органи);

6) брати активну участь у групах, що здійснюють обмін інформацією в сфері кіберризиків, уключаючи державні та міжнародні групи для збору, поширення та оцінки інформації про кіберзагрози та раннє попередження про них;

7) розробити та впровадити для працівників платіжних систем протоколи обміну інформацією щодо кіберзагроз, кіберінцидентів, кібератак тощо, що встановлюють їх обов'язки та відповідальність;

8) виявляти прогалини в установленому механізмі обміну інформацією та вживати заходів для їх усунення й сприяння налагодженню дієвого обміну інформацією у разі масштабної кібератаки.

XII. Навчання персоналу в сфері забезпечення кіберстійкості платіжної інфраструктури

77. Кіберстійкість платіжної інфраструктури залежить:

від спроможності об'єкта платіжної інфраструктури розвивати підходи та заходи, спрямовані на забезпечення кіберстійкості платіжної інфраструктури в умовах постійного розвитку кіберризиків та кіберзагроз;

від загальної культури управління ризиками в платіжній інфраструктурі, що досягається шляхом постійного навчання та розвитку в цій сфері.

78. Об'єкту платіжної інфраструктури рекомендується здійснювати такі заходи, пов'язані з навчанням та розвитком персоналу:

1) забезпечувати можливості для збору та аналізу інформації про поширені вразливості, кіберзагрози та кіберінциденти, що відбуваються як у межах екосистеми платіжної інфраструктури так і за її межами, та оцінки її потенційного впливу на платіжну інфраструктуру;

2) здійснювати аналіз отриманої інформації, визначати заінтересованих осіб, якими вона може бути використана з метою підвищення кіберстійкості платіжної інфраструктури, та забезпечувати передавання такої інформації;

3) проводити навчання всього персоналу (у тому числі керівників) щодо політики підтримки кібербезпеки платіжної інфраструктури та повідомлення про кіберінциденти та кібератаки щонайменше один раз на рік;

4) забезпечити наявність програм для навчання та підвищення кваліфікації персоналу, в тому числі керівників, у сфері кіберстійкості та їх постійне оновлення й удосконалення з урахуванням отриманого досвіду та знань;

5) включити до програми щорічного навчання з кіберстійкості питання щодо реагування на кіберінцидент, поточні кіберзагрози [наприклад, фішинг, цільовий фішинг (фішинг, спрямований на конкретну особу/групу осіб, що передбачає використання раніше отриманих персональних даних), соціальна інженерія)], порядку повідомлення про нетипову активність;

6) забезпечити виготовлення (створення) та поширення спеціальних навчальних матеріалів для працівників після виникнення суттєвих кіберінцидентів;

7) брати участь у навчальних заходах у сфері кіберризиків державного та міжнародного рівня;

8) установити показники для вимірювання та контролю ефективності впровадження стратегії забезпечення кіберстійкості (наприклад, частка працівників, що пройшла спеціальне навчання від загальної кількості працівників, частка кіберінцидентів від загальної кількості інцидентів, про які було повідомлено в установленому порядку в установлений строк) та щорічно здійснювати моніторинг зміни їх значення;

9) упровадити заходи, за допомогою яких здійснюється перевірка знань та розуміння персоналом їх відповідальності та ролі у збереженні кібербезпеки платіжної інфраструктури;

10) залучати критично важливий персонал із високим рівнем уразливості до кіберзагроз, кіберінцидентів та/або кібератак до навчання та тренувань;

11) проводити необхідне навчання та ознайомлення з операційними процедурами персоналу, який працюватиме з новими інформаційними системами, до початку експлуатації таких систем;

12) включити питання, пов'язані з кіберстійкістю та кібербезпекою платіжної інфраструктури до програми навчання, передбаченої для нових працівників;

13) активно відслідковувати технологічний розвиток та нові процеси управління кіберризиками та розглядати можливість придбання продуктів нових технологій, що можуть бути застосовані для підвищення кіберстійкості платіжної інфраструктури;

14) застосовувати знання та досвід, отримані внаслідок кіберінцидентів/кібератак, що вже відбулися, для удосконалення управління кіберризиком та удосконалення плану(ів) реагування, поновлення та відновлення діяльності платіжної інфраструктури;

15) здійснювати аналіз та порівнювати результати перевірок, тестів та інцидентів;

16) установити ефективність включення питань до програм навчання;

17) постійно відслідковувати прогрес у розвитку кіберстійкості.